



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002033760 A**(43) Date of publication of application: **31.01.02**

(51) Int. Cl. **H04L 12/54**
H04L 12/58
G06F 13/00
H04L 9/10
H04L 12/22

(21) Application number: **2000214624**(71) Applicant: **NEC CORP**(22) Date of filing: **14.07.00**(72) Inventor: **AZUMA TOMIHIKO**

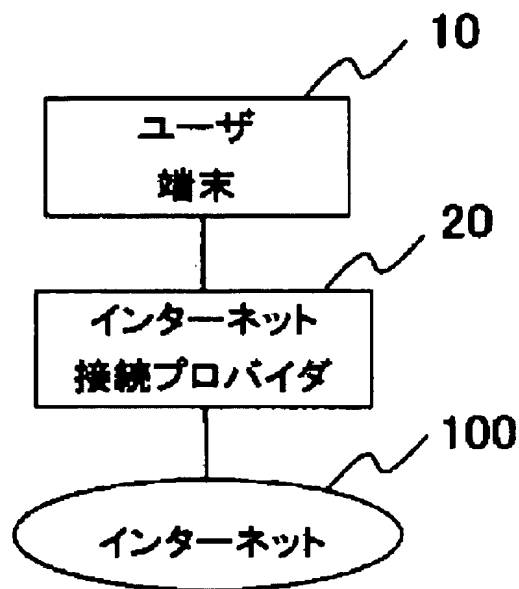
(54) **METHOD AND SYSTEM FOR
 SURROGATE-WARRANTING SECURITY OF
 ELECTRONIC MAIL, AND RECORDING MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a system and a method that can warrant the security of electronic mails in the Internet, independently of the presence/the absence of installing a security function into clients, such as user terminals.

SOLUTION: An internet connection provider 20 providing a service to connect a user terminal 10 to the Internet 100 has a means that carries out, in behalf of the user, processings required for security management, such as encryption of an electronic mail sent from the user terminal to the Internet, attachment of a signature to the electronic mail, inspection of presence of falsification of the signature-attached encryption mail from the Internet and its decoding.

COPYRIGHT: (C)2002,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-33760
(P2002-33760A)

(43) 公開日 平成14年1月31日 (2002.1.31)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 12/54		G 0 6 F 13/00	6 1 0 S 5 J 1 0 4
12/58		H 0 4 L 11/20	1 0 1 B 5 K 0 3 0
G 0 6 F 13/00	6 1 0	9/00	6 2 1 Z
H 0 4 L 9/10		11/26	
12/22			

審査請求 有 請求項の数9 O L (全 8 頁)

(21) 出願番号 特願2000-214624(P2000-214624)

(22) 出願日 平成12年7月14日 (2000.7.14)

(71) 出願人 000004237

日本電気株式会社
東京都港区芝五丁目7番1号

(72) 発明者 東 富彦

東京都港区芝五丁目7番1号 日本電気株
式会社内

(74) 代理人 100080816

弁理士 加藤 朝道

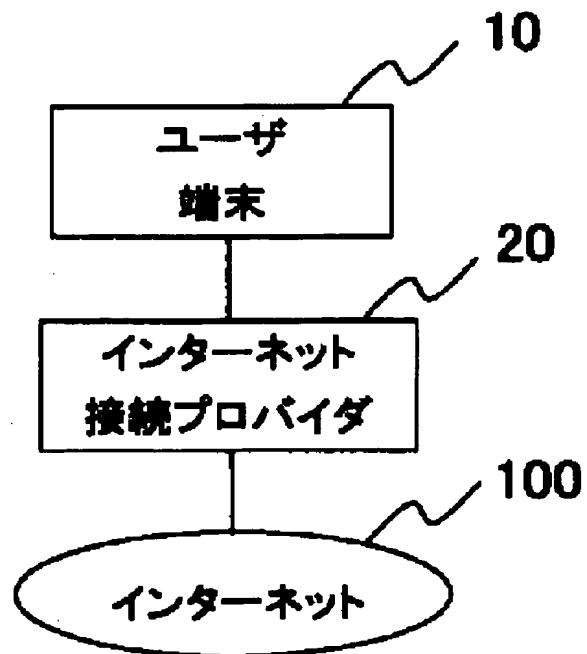
Fターム(参考) 5J104 AAD1 AA09 JA21 LA03 LA05
LA06 NA12 PA08
5K030 GA15 HA06 HCD1 JT02 LD19

(54) 【発明の名称】 電子メールのセキュリティを代行して保証する方法及びシステム並びに記録媒体

(57) 【要約】

【課題】 ユーザ端末等クライアント側のセキュリティ機能の実装の有無に依存することなく、インターネットにおける電子メールのセキュリティを確保可能とするシステム及び方法の提供。

【解決手段】 ユーザ端末10をインターネット100へ接続するサービスを提供するインターネット接続プロバイダ20に、ユーザ端末からインターネットへ送信する電子メールの暗号化と署名の添付、及び前記インターネットからの署名付き暗号メールの改竄の有無の検査と復号化など、セキュリティ管理に必要な処理を代行する手段を備える。



【特許請求の範囲】

【請求項1】ユーザ端末をインターネットへ接続するサービスを提供するインターネット接続プロバイダが、前記ユーザ端末から前記インターネットへ送信する電子メールの暗号化と署名の添付、及び、前記インターネットからの署名付き暗号メールの改竄の有無の検査と復号化を含む、セキュリティ管理に必要な処理を代行する手段を備えた、ことを特徴とする電子メールのセキュリティ代行システム。

【請求項2】ユーザ端末をインターネットに接続するサービスを提供するインターネット接続プロバイダが、電子メールのセキュリティを前記ユーザ端末に代行して行う代行手段として、

前記ユーザ端末から受け取った電子メールを暗号化し署名を添付して前記インターネットへ送出する手段と、署名付きで暗号化された電子メールが前記インターネットから送信されてきた場合に、前記電子メールの改竄の有無を検出し、改竄されていない場合に、前記暗号化された電子メールを復号する手段と、

を備え、前記ユーザ端末などの種類やセキュリティ機能の実装の有無に依存することなく、インターネットにおける電子メールのセキュリティを確保可能としたことを特徴とする電子メールのセキュリティ代行システム。

【請求項3】ユーザ端末をインターネットに接続するサービスを提供するインターネット接続プロバイダが、電子メールのセキュリティを前記ユーザ端末に代行して行う代行手段として、

前記ユーザ端末から受け取った平文の電子メールに対して、電子メール受信者だけが前記電子メールを復号化できるように暗号化する手段と、

前記暗号化された電子メールに、電子メール発信者の署名を付けて、前記インターネットへ、署名済みの暗号化された電子メールを送出する手段と、

署名付きの暗号化された前記ユーザ端末宛の電子メールが前記インターネットを通して送信されてきた場合に、前記電子メールが改竄されていないかどうかをチェックする手段と、

前記電子メールが改竄されていない場合には、前記暗号化メールを復号化し平文メールとする手段と、

前記ユーザ端末から受信メールを要求した場合に、復号化した平文のメールをユーザ端末に配送するメール配送手段と、

を備え、

前記電子メールが改竄されている場合には、前記電子メールの受信を廃棄する、ことを特徴とする電子メールのセキュリティ代行システム。

【請求項4】ユーザ端末をインターネットに接続するサービスを提供するインターネット接続プロバイダのサーバ装置が、

電子メールアドレスと該電子メールアドレスに対応する

秘密鍵との組を記憶した秘密鍵記憶手段と、

電子メールアドレスと該電子メールアドレスに対応する公開鍵との組を記憶している公開鍵記憶手段と、を備え、

前記秘密鍵は、電子メールに対して発信者の署名を付ける場合と、送信されてきた暗号化メールを復号化する場合に使用され、

前記公開鍵は、電子メールの宛先に指定された電子メールアドレスのユーザにしか読めないようにメールを暗号化する場合と、メールが改竄されていないかどうかをチェックする場合に使用され、

電子メールの宛先の電子メールアドレスに対応する公開鍵を前記公開鍵記憶部から取得し、前記ユーザ端末から受け取った平文メールを公開鍵で暗号化するメール暗号化手段と、

電子メール発信者の電子メールアドレスに対応する秘密鍵を前記秘密鍵記憶部から取得し、前記電子メールのメッセージダイジェストを計算し、その値を、前記秘密鍵で暗号化した上で電子メールに発信者の署名として添付するメール署名添付手段と、

前記インターネットから送信されてきた署名付きで暗号化された電子メールに対して、電子メール発信者の電子メールアドレスに対応する公開鍵を前記公開鍵記憶部から取得し、前記電子メールに添付されている署名を前記公開鍵で復号化し、署名の値と電子メールのメッセージダイジェストとを比較することによって、メールが改竄されていないかどうかを検査するメール署名検査手段と、

改竄されていない電子メールについて、該電子メールの宛先の電子メールアドレスに対応する秘密鍵を前記秘密鍵記憶部から取得し、暗号化されている電子メールを前記秘密鍵で復号化するメール復号化手段と、

前記ユーザ端末から受信メールを要求した場合に、復号化した平文のメールをユーザ端末に配送するメール配送手段と、

を備えたことを特徴とするサーバ装置。

【請求項5】ユーザ端末をインターネットに接続するサービスを提供するインターネット接続プロバイダにおける電子メールのセキュリティ管理方法であって、

前記ユーザ端末から前記インターネットへ送信する電子メールの暗号化と署名の添付、及び、前記インターネットから前記ユーザ端末宛の電子メールの改竄の有無の検査と復号化を含む、電子メールのセキュリティ管理に必要な処理を、前記インターネットの接続点に配置されたインターネット接続プロバイダが代行して行うことで、ユーザ端末などの種類やセキュリティ機能の実装の有無に依存することなく、インターネットにおける電子メールのセキュリティを確保可能としたことを特徴とする、電子メールのセキュリティ管理方法。

【請求項6】ユーザ端末をインターネットに接続するサ

ービスを提供するインターネット接続プロバイダにおいて、電子メールのセキュリティを前記ユーザ端末に代行して行うサーバを配置し、

前記ユーザ端末からの平文の電子メールに対して、電子メール受信者だけが前記電子メールを復号化できるように暗号化し、

さらに電子メール発信者の署名を付けてインターネットへ署名済みの暗号化された電子メールを送出し、

署名済みの暗号化された前記ユーザ端末宛の電子メールが前記インターネットを通して前記サーバに送信されてきた場合に、前記電子メールの改竄の有無をチェックし、

前記電子メールが改竄されていない場合には、暗号化されている前記電子メールを復号化して、平文メールにした上で、メール受信要求のあった前記ユーザ端末へ配送し、

一方、前記電子メールが改竄されている場合には前記電子メールの受信を拒否する、ことを特徴とする電子メールのセキュリティ管理方法。

【請求項7】ユーザが、ユーザ端末で電子メールを作成し、該電子メールを平文のままインターネット接続プロバイダに送信するステップと、

前記インターネット接続プロバイダにおいて前記ユーザ端末から送信された電子メールを受信し、前記電子メールの宛先の電子メールアドレスに対応する公開鍵を、電子メールアドレスと該電子メールアドレスに対応する公開鍵との組を記憶している公開鍵記憶部から取得し、前記平文の電子メールを公開鍵で暗号化するステップと、前記電子メールの発信者の電子メールアドレスに対応する秘密鍵を、電子メールアドレスと該電子メールアドレスに対応する秘密鍵との組を記憶した秘密鍵記憶部から取得し、前記電子メールのメッセージダイジェストを計算し、その値を秘密鍵で暗号化した上で、前記電子メールに、発信者の署名として添付するステップと、前記インターネット接続プロバイダから、署名付き暗号化メールを、インターネットへ送出するステップと、を含む、ことを特徴とする電子メールのセキュリティ管理方法。

【請求項8】前記インターネット接続プロバイダが、前記インターネットから、署名付きの暗号化された電子メールを受信するステップと、

電子メール発信者の電子メールアドレスに対応する公開鍵を前記公開鍵記憶部から取得し、前記電子メールに添付されている署名を公開鍵で復号化するステップと、前記署名の値と前記電子メールのメッセージダイジェストとを比較することによって、前記電子メールが改竄されていないかどうかを検査するステップと、

前記電子メールが改竄されていない場合には、前記電子メールの宛先のメールアドレスに対応する秘密鍵を前記秘密鍵記憶部から取得し、暗号化されている前記電子メ

ールを秘密鍵で復号化するステップと、

前記ユーザ端末から受信メールを要求した場合に、前記復号化した平文の電子メールをユーザ端末に配送するステップと、

を含む、ことを特徴とする請求項7記載の電子メールのセキュリティ管理方法。

【請求項9】ユーザ端末をインターネットに接続するサービスを提供するインターネット接続プロバイダのサーバ装置において、

10 電子メールアドレスと、それに対応する秘密鍵との組を記憶した秘密鍵記憶部と、

電子メールアドレスと、それに対応する公開鍵との組を記憶している公開鍵記憶部を備えた記憶装置を備え、

前記秘密鍵は、電子メールに対して発信者の署名を付ける場合と、インターネットから送信されてきた暗号化メールを復号化する場合に使用され、

前記公開鍵は、電子メールの宛先に指定された電子メールアドレスのユーザにしか読めないように電子メールを暗号化する場合と、電子メールが改竄されていないかどうかをチェックする場合に使用され、

20 (a) 前記ユーザ端末から受け取った平文の電子メールの宛先の電子メールアドレスに対応する公開鍵を前記公開鍵記憶部から取得し、前記平文の電子メールを公開鍵で暗号化するメール暗号化処理と、

(b) 電子メール発信者の電子メールアドレスに対応する秘密鍵を前記秘密鍵記憶部から取得し、前記電子メールのメッセージダイジェストを計算し、その値を、秘密鍵で暗号化した上で電子メールに発信者の署名として添付するメール署名添付処理と、

30 (c) 前記インターネットから送信されてきた署名付きで暗号化された電子メールに対して、電子メール発信者の電子メールアドレスに対応する公開鍵を前記公開鍵記憶部から取得し、前記電子メールに添付されている署名を公開鍵で復号化し、前記署名の値と、電子メールのメッセージダイジェストとを比較することによって、メールが改竄されていないかどうかを検査するメール署名検査処理と、

(d) 前記電子メールの宛先の電子メールアドレスに対応する秘密鍵を前記秘密鍵記憶部から取得し、暗号化されている電子メールを秘密鍵で復号化するメール復号化処理と、

40 (e) 前記ユーザ端末から受信メールを要求した場合に、前記復号化した平文の電子メールを前記ユーザ端末に配送するメール配送処理と、

の前記(a)乃至(e)の処理を前記サーバ装置を構成するコンピュータに実行させるためのプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

50 【発明の属する技術分野】本発明は、電子メールのメー

ルのセキュリティを確保するシステム及び方法並びにプログラムを記録した記録媒体に関する。

【0002】

【従来の技術】電子メールのセキュリティを確保するためのシステムとしては、暗号化したメッセージをMIME形式で転送するS/MIME (Secure/Multipurpose Internet Mail Extension; エスマイム; RSAデータセキュリティ社開発)、PGP (Pretty Good Privacy; ビジービー; PGP社が開発した暗号化プログラム、メールの内容を送信相手の公開鍵で暗号化して送信する)等のセキュリティ機能を具備したメールクライアントが広く一般的に利用されている。

【0003】セキュリティを有効に機能させるためには、自分の秘密鍵や送信相手のデジタル証明書等を、自分が使用する端末に事前にインストールする方法が、一般的に採用されている。

【0004】

【発明が解決しようとする課題】しかしながら、従来のシステムは、次のような問題点を有している。

【0005】メールを送受信する端末が、従来のPC (パーソナルコンピュータ) から、携帯電話機や、携帯情報端末、FAX (ファクシミリ)などの端末へ広がるとともに、セキュリティ機能を備えたメールクライアントを持たない端末が増加し、インターネット上でのメールのセキュリティを確保することができなくなっていることである。

【0006】そして、急速に普及している携帯電話においては、端末側でのセキュリティ機能の実装が困難であり、このため、ビジネスでの利用を妨げる大きな原因ともなっている。

【0007】したがって、本発明は、上記問題点に鑑みてなされたものであって、その目的は、ユーザ端末等クライアント側のセキュリティ機能の実装の有無に依存することなく、インターネットにおける電子メールのセキュリティを確保可能とするシステム及び方法並びに記録媒体を提供することにある。

【0008】

【課題を解決するための手段】前記目的を達成する本発明は、ユーザ端末をインターネットへ接続するサービスを提供するインターネット接続プロバイダに、前記ユーザ端末から前記インターネットへ送信する電子メールの暗号化と署名の添付、及び前記インターネットからの署名付き暗号メールの改竄の有無の検査と復号化など、セキュリティ管理に必要な処理を代行するものである。

【0009】

【発明の実施の形態】本発明の実施の形態について説明する。本発明は、電子メールの機能をユーザに提供しているインターネット接続プロバイダ (ISP) が、ユーザに代わって、電子メールの暗号化及び復号化や、署名の添付、改ざん (改竄) の検出を実行することにより、

ユーザが利用するメールクライアントや、ユーザ端末などの種類およびセキュリティ機能の実装の有無に依存することなく、インターネットにおける電子メールのセキュリティ確保を実現するものである。

【0010】より詳細には、本発明は、その好ましい一実施の形態において、図1を参照すると、ユーザはインターネット接続プロバイダ20に加入しており、ユーザはインターネット接続プロバイダ20から電子メールアドレスが割り当てられている。ユーザは、ユーザ端末10を利用してインターネット接続プロバイダ20に接続し、署名も暗号化もされていない平文メールを、インターネット接続プロバイダ20に送信する。

【0011】インターネット接続プロバイダ20は、平文メールに対して、メール受信者だけがメールを復号化できるように暗号化し、メール発信者の署名を付けて、インターネット100へ、署名済み暗号化メールとして、送出する。

【0012】署名済み暗号化メールがインターネット100を通して、インターネット接続プロバイダ20に配送されてきた場合、インターネット接続プロバイダ20は、メールが改竄されていないかどうかをチェックする。

【0013】チェックの結果、メールが改竄されていない場合には、インターネット接続プロバイダ20は、暗号化メールを復号化して、平文メールにした上で保存する。

【0014】一方、メールが改竄されている場合には、インターネット接続プロバイダ20は、メールの受信を拒否し、改竄されたメールがユーザに配送されることを防止する。

【0015】ユーザは、ユーザ端末10を利用してインターネット接続プロバイダ20に接続し、インターネット100上で改竄されていないことが保証されている平文のメールを受け取る。

【0016】

【実施例】上記した本発明の実施の形態についてさらに詳細に説明すべく、本発明の実施例について図面を参照して以下に説明する。図1は、本発明の一実施例のシステム構成を示す図である。図1を参照すると、本発明の一実施例は、ユーザ端末10と、インターネット接続プロバイダ20と、インターネット100とを備えて構成されている。

【0017】ユーザ端末10は、インターネット接続プロバイダ20を介して、インターネット100へ接続できる機能を備えた端末よりなり、例えば携帯電話端末、携帯情報端末、あるいはパーソナルコンピュータ等よりなる。

【0018】ユーザ端末10は、インターネット接続プロバイダ20を介して、電子メールを送受信する機能と、インターネット接続プロバイダ20へ有線あるいは

無線により、相互に接続できる機能を備えている。

【0019】インターネット接続プロバイダ20は、あらかじめ登録されているユーザに対して、インターネット100への電子メールの受発信サービス（メールサーバ）を提供しており、サーバ等の情報処理装置によって構成されている。

【0020】インターネット接続プロバイダ20を介したインターネット100への電子メールの受発信サービスは、事前にユーザ登録したユーザだけが利用することができる。

【0021】図2は、本発明の一実施例におけるインターネット接続プロバイダ20のサーバ装置の構成の一例を示す図であり、データ処理装置21と、記憶装置22とを備えている。インターネット接続プロバイダ20は、

- ・ユーザに対して電子メールアドレスを割り当て、電子メールを暗号化したり、署名したりするための情報を生成する機能と、
 - ・電子メールアドレスと暗号化に必要な情報を組にして記憶する機能と、
 - ・電子メールアドレスと署名を付けるために必要な情報を組にして記憶する機能と、
- を有する。

【0022】電子メールを暗号化したり署名したりするための情報としては、秘密鍵と共通鍵のペアなどがある。

【0023】より詳細には、インターネット接続プロバイダ20のサーバ装置を構成するデータ処理装置21は、ユーザがユーザ端末10を利用して発信した、暗号化も署名もされていない電子メールに対して、宛先に指定されている受信者だけが電子メールを読めるように暗号化するメール暗号化手段211と、発信者の署名を付けた上で、インターネット100に送出するメール署名添付手段213と、インターネット100から受信した電子メールが改竄されていないかどうかを検査する機能を有し、改竄されている場合にはメールを破棄し、ユーザを改竄されたメールから保護するメール署名検査手段214と、暗号化されている電子メールを復号化して平文メールとして保存するメール復号手段212と、ユーザがユーザ端末10から受信メールを要求した場合に、復号化した平文のメールをユーザ端末に配送するメール配送手段215と、を有する。サーバ装置の記憶装置22は、電子メールアドレスと該電子メールアドレスに対応する秘密鍵との組を記憶した秘密鍵記憶部221と、電子メールアドレスと該電子メールアドレスに対応する公開鍵との組を記憶している公開鍵記憶部222と、を備えている。秘密鍵は、電子メールに対して発信者の署名を付けるメール署名添付手段213と、送信されてきた暗号化メールを復号化するメール復号手段212で使用され、公開鍵は、電子メールの宛先に指定された電子

メールアドレスのユーザにしか読めないようにメールを暗号化するメール暗号化手段211と、メールが改竄されていないかどうかをチェックするメール署名検査手段214で、使用される。

【0024】インターネット接続プロバイダ20のサーバ装置の上記手段211～215は、サーバを構成するデータ処理装置21でプログラムを実行することで実現される。この場合、該プログラムを記録した記録媒体（磁気ディスク、磁気テープ、光ディスク、あるいは半導体メモリ等）から該プログラムをデータ処理装置21に読み出して実行することで、本発明に係るインターネット接続プロバイダのサーバ装置を実施することができる。

【0025】次に図1乃至図6を参照して、本発明の一実施例の動作について詳細に説明する。

【0026】図3は、本発明の一実施例において、ユーザ端末10からのメール送信時の動作を説明する流れ図である。まずユーザ端末10からのメール送信時の動作について詳細に説明する。

【0027】ユーザはユーザ端末10を利用してメールを作成し、平文のままインターネット接続プロバイダ20に送信する（ステップA1）。

【0028】インターネット接続プロバイダ20は、平文メールを受信し、メールの宛先のメールアドレスに対応する公開鍵で暗号化する（ステップA2）。

【0029】図6は、インターネット接続プロバイダ20の公開鍵記憶部222に記憶されているメールアドレスと公開鍵の組情報の一例を示す図である。

【0030】メールの宛先のメールアドレスが、"u-suzuki@abc.com"である場合には、対応する公開鍵として"111...001"が暗号化に利用される。

【0031】次に、インターネット接続プロバイダ20は、メール発信者のメールアドレスに対応する秘密鍵を利用してメールに署名する（図3のステップA3）。

【0032】署名の方法としては、メールのメッセージダイジェスト（ハッシュ値）を計算し、その値を秘密鍵で暗号化した上でメールに添付する方法などがある。

【0033】図5は、インターネット接続プロバイダ20の秘密鍵記憶部221に記憶されているインターネット接続プロバイダ20が記憶しているメールアドレスと秘密鍵の組情報の一例を示す図である。

【0034】メール発信者のメールアドレスが"t-azuma@biglobe.ne.jp"である場合には、対応する秘密鍵として"101...001"が署名に利用される。

【0035】最後にインターネット接続プロバイダ20は署名付き暗号化メールをインターネット100へ送り出す（図3のステップA4）。

【0036】図4は、本発明の一実施例において、インターネット100から署名付き暗号化メールを受信した場合の動作を説明するための流れ図である。図4を参照

して、インターネット100から署名付き暗号化メールを受信した場合の動作について詳細に説明する。

【0037】インターネット接続プロバイダ20はインターネット100から署名付き暗号化メールを受信する(ステップB1)。

【0038】インターネット接続プロバイダ20は、メール発信者のメールアドレスに対応する公開鍵を利用して、メールに添付されている署名を公開鍵で復号化し(ステップB2)、署名の値とメールのメッセージダイジェスト(ハッシュ値)とを比較することによって、メールが改竄されていないかどうかを検査する(ステップB3)。

【0039】図6に示す例では、メール発信者のメールアドレスが"u-suzuki@abc.com"である場合には、対応する公開鍵として"111...001"が署名の復号化に利用される。メールが改竄されていない場合には、インターネット接続プロバイダ20はメールの宛先のメールアドレスに対応する秘密鍵を利用して、暗号化されているメールを秘密鍵で復号化し保存する(ステップB4)。

【0040】図5に示す例では、メール受信者のメールアドレスが"t-azuma@biglobe.ne.jp"である場合には、対応する秘密鍵として"101...001"が暗号化メッセージの復号化に利用される。

【0041】メールが改竄されている場合には、インターネット接続プロバイダ20はメールの受信を拒否し、改竄されたメールがユーザに届くのを防止する(図4のステップB5)。

【0042】インターネット接続プロバイダ20は、ユーザ端末10からメールの要求があった場合に平文メールをメールクライアント返却する(ステップB7)。

【0043】ユーザはユーザ端末10を利用してインターネット接続プロバイダ20に対して受信したメールを要求し(ステップB6)、インターネット接続プロバイダ20から平文メールを受け取る(ステップB8)。

【0044】

【発明の効果】以上説明したように、本発明によれば下記記載の効果を奏する。

【0045】本発明の第1の効果は、電子メールを送受信するユーザ端末に、特別なソフトや装置を組みこむことなく、インターネット上での電子メールのセキュリティを確保することができる、ということである。

【0046】近時、特に急速に普及している携帯電話や携帯情報端末などをメールクライアントの端末として利用できるインターネット接続プロバイダにおいては、

- ・対象とする機種が多様多様であること、
- ・既に出荷されている台数が膨大であること、

から、インターネット接続プロバイダ上で電子メールのセキュリティ管理を行う本発明は、セキュリティ向上に顕著なる効果を奏する。

【0047】その理由は、本発明においては、電子メールのセキュリティを確保するために必要な処理をユーザ端末側に持たせるのではなく、インターネットとの接続点を持つインターネット接続プロバイダがすべて代行する構成とされており、ユーザ端末とインターネット接続プロバイダを結ぶ有線および無線のネットワークは、一般的にインターネット上に比べてセキュリティの脅威ははるかに少ないため、インターネットと接続しているポイントに、セキュリティの機能を集約させることができるようにした、ためである。

【0048】本発明の第2の効果は、セキュリティ確保に必要な管理コストを大幅に低減することができる、ということである。特に、複数の端末を使うユーザにとっては、端末ごとにセキュリティの設定をする必要がなくなるため効果は顕著である。

【0049】その理由は、本発明においては、セキュリティ確保に必要な秘密鍵や公開鍵などをインターネット接続プロバイダで一元管理することにより、ユーザ端末毎のセキュリティ設定を不要としている、ためである。

【図面の簡単な説明】

【図1】本発明の一実施例のシステム構成を示す図である。

【図2】本発明の一実施例におけるISPのサーバの構成の一例を示す図である。

【図3】本発明の一実施例において、ユーザ端末からのメール送信時の動作を説明するための流れ図である。

【図4】本発明の一実施例において、インターネットから署名付き暗号化メールを受信した場合の動作を説明するための流れ図である。

【図5】本発明の一実施例における秘密鍵記憶部に記憶されている電子メールアドレスと秘密鍵の組情報の例を示す図である。

【図6】本発明の一実施例における公開鍵記憶部に記憶されている電子メールアドレスと公開鍵の組情報の例を示す図である。

【符号の説明】

10 ユーザ端末

20 インターネット接続プロバイダ

100 インターネット

21 データ処理装置

22 記憶装置

211 メール暗号化手段

212 メール復号化手段

213 メール署名添付手段

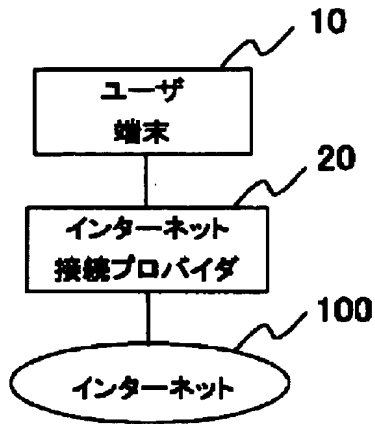
214 メール署名検査手段

215 メール配送手段

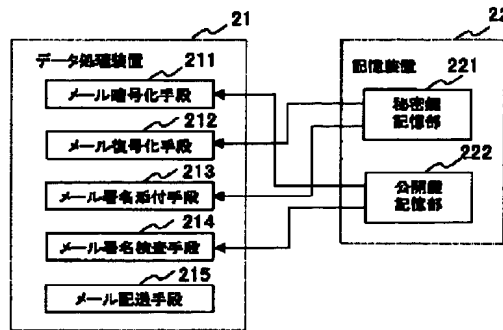
221 秘密鍵記憶部

222 公開鍵記憶部

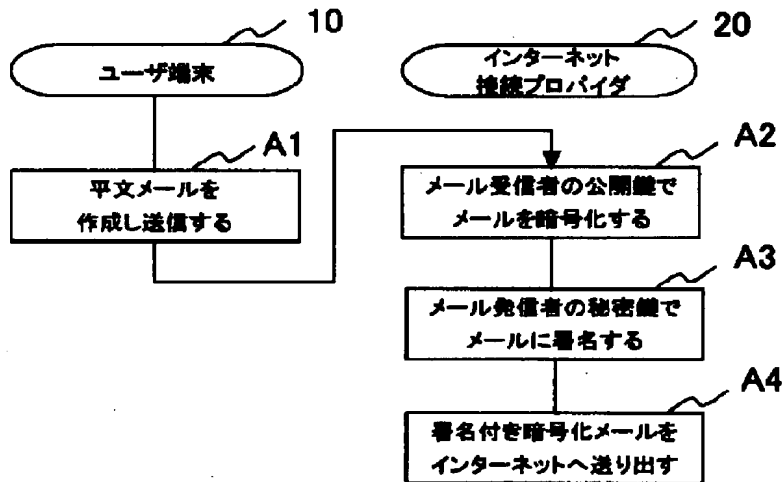
【図1】



【図2】



【図3】



【図5】

電子メールアドレス	秘密鍵
t-azuma@biglobe.ne.jp	101...001
h-kubota@biglobe.ne.jp	100...100
...	...

【図6】

電子メールアドレス	公開鍵
t-azuma@biglobe.ne.jp	110...011
h-kubota@biglobe.ne.jp	101...110
u-suzuki@abc.com	111...001
i-sato@nec.co.ne	111...101
...	...

【図4】

